GE Healthcare

Hugh Zettel
Director, Government & Industry Relations

9900 Innovation Drive, RP2142
Wauwatosa, WI 53226

T 414-721-2015
hubert.zettel@ge.com

June 4, 2007

Mr. Steven Posnack
Office of the National Coordinator
330 C Street, SW, Suite 4090
Washington, DC 20201

Dear Mr. Posnack:

GE Healthcare (GEHC) appreciates the opportunity to respond to the American Health Information Community Confidentiality, Privacy and Security Workgroup's request for feedback on its working hypothesis to protect electronic health information in a nationwide health information exchange environment. As a leading supplier of health information technology, diagnostic imaging, diagnostics and services solutions to the global healthcare market, we believe that our experience in ensuring the security and privacy of health information for our customers provides us with helpful insights in improving security and privacy policies. Given the limited time to respond to the request for information, are initial responses are provided below, and will be willing to provide more detail upon request.

The working hypothesis posed by the CPS workgroup is as follows: *All persons and entities excluding consumers that participate in an electronic health information exchange network at a local, state, regional, nationwide level, through which individually identifiable electronic health information is stored, compiled, transmitted, or accessed, should be required to meet privacy and security criteria at least equivalent to relevant Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule requirements.*

1. Enforceable mechanisms

- GEHC recommends that several aspects of the current HIPAA rule should be clarified, which would make the existing rules easier to enforce, specifically as they relate to Auditing Guidelines. GEHC recommends that several aspects of the current HIPAA rule should be clarified, which would make the existing rules easier to enforce, specifically as they relate to Auditing Guidelines. For example, if a physician reads an email from a patient and uses some of that information to provide clinical care, what should be captured to meet auditing requirements under HIPAA; the entire email, the relevant portion of the email, or a reference to the patient's email?
- In a health information exchange world, it is important that unambiguous rules be established for all entities exchanging electronic information, to create a level playing field and a consistent, clear set of expectations that everyone will be held accountable to. For example, the healthcare electronic data interchange industry (EDI) gets certified under a consistent set of processes by the Electronic Healthcare Network Accreditation Commission EHNAC (see www.ehnac.org).
- Mechanisms must be established to recognize the variety of entities that will be connected to a health information exchange (HIE), and reflect that there will be ongoing improvements in security technology that will enhance privacy policies over time.
- Protected Health Information (PHI) breaches are predominantly "inside jobs", not a result of the presence of an HIE network. Therefore we recommend additional emphasis be placed on individual accountability, as well increased oversight by the Department of Health and Human Services to increase the deterrent effect.
- GEHC encourages the CPS workgroup to give thoughtful consideration to the Health Information Security and Privacy Collaborative (HISPC), which has provided a forum to harmonize state security and privacy regulations in anticipation of the emerging HIE environment. Many of the state proposals offer pragmatic suggestions towards

harmonization of disparate state regulations and are aligned with improvements to the existing HIPAA regulation.

- GEHC suggests that CPS consider the global implications of the 'working hypothesis', whether it's related to patients that seek care outside the borders of our country, or relative to suppliers that provide services to covered entities that may not be located in the United States.
- GEHC suggests CPS clarify the 'working hypothesis' to consider components in the exchange of individually identifiable health information (IIHI) that may be thought of as only "conduits" to move information, but not act on it. For example, ePrescribing middleware vendors may be thought of as a conduit between the prescribing physician and the retail pharmacy.

2. Relevant requirements

- Everyone involved in the information exchange environment is either a Covered Entity (CE) or a Business Associate (BA) (w/ the exclusion of conduits), and HIPAA addresses the protections that should apply to these entities. The scope could be clearer as to who would be covered under this ~ All Entities (including conduits) that's involved in the process and transaction of sensitive data. Aside: HIPAA requires CE to obtain written confidentiality assurances from business associates: it defines how BAs must use or release IIHI (safeguards i.e. authentication), immediate reporting of successful breaches, and promises to protect and return & destroy, and assurance to make info available for compliance purposes.
- Everyone involved in the information exchange environment is either a Covered Entity (CE) or a Business Associate (BA) (w/ the exclusion of conduits), and HIPAA addresses the protections that should apply to these entities. A RHIO is neither a covered entity nor a business associate, but the entities that make up the RHIO, whether a covered entity, business associate, or conduit of PHI, should implement relevant and acceptable industry standards such as ISO17799, *Information technology - Security techniques - Code of practice for information security management*; and ISO 27799 - Security Management in Health using ISO/IEC 17799.

- The 'working hypothesis' states that those that touch PHI should be required to meet privacy & security criteria at least equivalent to HIPAA; which is not clear (Covered Entity or Business Associate requirements). If we hold all the entities to the CE standards we would have to carve out some of the non-applicable responsibilities, such that are required of CE that has direct patient contact (ex. Notice of Privacy Practice, Individual Rights, Uses & Disclosures of PHI for Underwriting, or Uses and Disclosures of PHI to personal representatives). Although, the Clearinghouse responsibilities as a CE could apply to all involved in this environment. Note that we want to be careful not to shift liability; ultimately it is the CE responsibility (since they are the data collectors) to assure the BA's compliance w/ the standards.
- GEHC recommends that HIPAA guidelines regarding consents and "minimum necessary" should be clarified given today's new health information exchange world, which would simplify governance and enhance enforcement. States involved in the HISPC process have made recommendations regarding enhancement of these two HIPAA guidelines, and we encourage the CPS Workgroup to review the state feedback.

3. Business Associates

Below are our responses given our role as a Business Associate:

A) How does you organization ensure compliance with the privacy and security policies of covered entities with whom it contracts, particularly when there are numerous contracts?

- We ensure compliance w/ the privacy & security policies of our customers contractually through a Business Associate Agreement (BAA), organizationally through appointing process owners (privacy focal points), implementing standard operating procedures & policies, trainings, and adhering to an incidence response process.

B) How do you handle business associate contracts with large numbers of covered entities including compliance with each covered entity's privacy policies?

- GEHC has a centralized process, and have adopted a global framework, or Global Acceptable Privacy Principles (GAPP), based on the Code of Fair Conduct. The elements of GAPP include:

    1. Scope & Impact / Protected information flow analysis
    2. Organizational arrangements
    3. Management system and standard operating procedures
    4. Regulatory requirements & reporting obligations
    5. Notice, choice & consent requirements
    6. Collection use & disclosure
    7. Transfers of regulated personal information
    8. Rights of data subjects
    9. Safeguards (security)
    10. Change control (new product/process introduction)
    11. Crisis management control procedures
    12. Monitoring & enforcement

- GEHC has established language in our commercial contracts, and although it is not our responsibility as a business associate to initiate the execution of a BAA, we try to take a proactive approach. If there are any negotiations it goes through the appropriate channels to assure compliance is possible under the negotiated language. All of GEHC has one signatory, the Chief Privacy Officer, and all executed BAAs are stored in a BAA database that is managed by GEHC legal.
- GEHC uses the common BAA developed jointly by the National Electronic Manufacturers Association (NEMA) and the American Hospital Association (AHA). We recommend that a collaborative, consensus based process be explored that uses this BAA to help reduce the number of BAA used for health information, or use the NEMA/AHA BAA as the starting point for creating a common health information exchange agreement. The sample BAA can be found at: www.nema.org/prod/med/security/upload/2002-10-31-Introduction_to_NEMA_HIPAA_BAA_Sample_Language.pdf.

C) How are business associate agreements negotiated? Do you have a standard contract?

- See answer to 4.B. Yes

D) How is the data protection compliance of subcontractors ensured and/or assessed?

- We assure compliance with our subcontractors by established language in our terms and conditions, having them execute a BAA, requesting their work instruction documentation or standard operating procedures, self auditing tools to assess their compliance, mitigation and reporting of incidents.

E) Do you have subcontractors and how do you handle those agreements?

- Yes, we have established language in our terms and conditions and a standard Vendor BAA that sets out their obligations with regard to use and disclosure of PHI.

F) How would direct accountability for meeting relevant HIPAA requirements impact your business?

- It would have a medium impact from having to formalize programs to meet prescribed requirements. Today we operate under a Framework of Generally Acceptable Privacy & Data Protection Principles.

4. General Questions

A) What are the implications of having some entities performing similar services covered by federal law (e.g., HIPAA) and others not? For example, a personal health record (PHR) could be offered by a health plan (covered entity) and an independent PHR service provider (non-covered entity). How does this impact your competitiveness?

- If non-covered entities handling PHRs where required to meet prescribed requirements than efficiency, effectiveness and cost could be affected due to controls necessary for compliance. Also, misinterpretation of controls or misapplication of controls would create bottlenecks in the flow of critical Healthcare data.

- Exchange of health information would be hindered since Covered Entities would be reluctant to share information by entities that not bound by the same level of accountability, as is the case today.
- Adding another party as an enforcement entity, such as the Federal Trade Commission for enforcement of non-covered entities only complicates an environment that already is fragmented by various federal and state privacy and security regulations.

ii. How does this impact your ability to exchange information with others?

- Significantly, particularly with suppliers and international entities.

iii. Does contracting with non-covered entities create different levels of accountability and/or enforceability in the exchange of health information?

- Non-covered entities may be restricted in fully participating in health information exchange due to Covered Entities reluctance to manage the risk of PHI breach.
- Governance within a HIE would have to establish some mechanism that provides the additional protections necessary to allow non-covered entities to participate in information exchange, and enforcement models would have to be consistent with those used by Covered Entities.

B) Assuming you are not a covered entity, what would be the implications of complying with enforceable confidentiality, privacy, and security requirements at least equivalent to relevant HIPAA principles?

- It would have a medium impact from having to formalize programs to meet prescribed requirements. Today, GEHC operates under a Framework of Generally Acceptable Privacy & Data Protection Principles. This affords some flexibility to enable and meet various customer requirements, but it still requires formalizing an agreement that may not be necessary if all parties were held accountable to the same policy.

C) Is there a minimum set of confidentiality, privacy, and security protections that you think everyone should follow, if not HIPAA, what?

- At a high level Code of Fair Information Practices and at a more granular level GAPP
- If we could modify the BAA as standard across all entities that touch this data, and attach specifications of process as an addendum, this would alleviate most of the negotiation and complication of the BAA process.
- With the increased global focus on security and privacy policy, GEHC suggests that the CPS workgroup consider adopting the Organization for Economic Co-operation and Development (OECD) International Data Protection Principles, which can provide a useful framework to enhance security standards that ensures health information privacy.
- GEHC recommends that entities that make up the RHIO, whether a covered entity, business associate, or conduit of PHI, should implement relevant and acceptable industry standards such as ISO17799, *Information technology - Security techniques - Code of practice for information security management*; and ISO 27799 - Security Management in Health using ISO/IEC 17799.

Thank you for allowing GE Healthcare to provide feedback on this very important healthcare policy matter. If you have any further questions, please contact Hugh Zettel at hubert.zettel@med.ge.com.

Regards,

Hugh Zettel
Director, Government & Industry Relations

cc Jackie Studer
Kim Tyrrell-Knott
Ericka Watson